(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年11 月7 日 (07.11.2002)

PCT

(10) 国際公開番号
WO 02/089426 A1

(51) 国際特許分類7: H04L 12/56

(21) 国際出願番号: PCT/JP02/04139

(22) 国際出願日: 2002 年4 月25 日 (25.04.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-133290 2001 年4 月27 日 (27.04.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・データ (NTT DATA CORPORATION) [JP/JP]; 〒135-6033 東京都 江東区 豊洲三丁目３番３号 Tokyo (JP). 株式会社 サイバー・ソリューションズ (CYBER SOLUTIONS INC.) [JP/JP]; 〒989-3204 宮城県 仙台市 青葉区南吉成六丁目６番地の３ ＩＣＲビル３Ｆ Miyagi (JP).

(72) 発明者; および

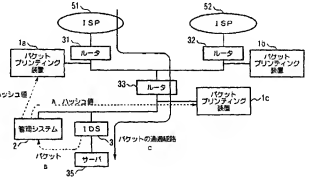
(75) 発明者/出願人 (米国についてのみ): 大谷 尚通 (OHTANI,Hisamichi) [JP/JP]; 〒135-6033 東京都 江東区 豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内 Tokyo (JP). 北條 武 (HOJO,Takeshi) [JP/JP]; 〒135-6033 東京都 江東区 豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内 Tokyo (JP). 岩田 恵一 (IWATA,Keiichi) [JP/JP]; 〒135-6033 東京都 江東区 豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内 Tokyo (JP). キニグレンマンスフィールド (KEENI,Glenn Mansfield) [IN/JP]; 〒989-3204 宮城県 仙台市 青葉区南吉成六丁目６番地の３ ICRビル3F 株式会社サイバー・ソリューションズ内 Miyagi (JP).

(74) 代理人: 志賀 正武 , 外(SHIGA,Masatake et al.); 〒169-8925 東京都 新宿区 高田馬場三丁目２３番３号 ＯＲビル Tokyo (JP).

[続葉有]

(54) Title: PACKET TRACING SYSTEM

(54) 発明の名称: パケット追跡システム



1a...PACKET PRINTING DEVICE
1b...PACKET PRINTING DEVICE
1c...PACKET PRINTING DEVICE
31...ROUTER
32...ROUTER
33...ROUTER
2...MANAGEMENT SYSTEM
35...SERVER
A...HASH VALUE
B...PACKET
C...ROUTE ALONG WHICH PACKET PASSES

(57) Abstract: A packet tracing system capable of tracing a packet even by using an existing network device. Packet printing devices (1a, 1b and 1c) create hash values from all the packets flowing in a network to be monitored, and stores the created hash values in a storage unit. An IDS (3) detects a questionable packet in the monitored network. On receiving a warning and a packet to be traced from the IDS (3), a management system (2) creates the hash value of the packet and transmits a search request containing the created hash value to the packet printing devices (1a, 1b and 1c). These devices (1a, 1b and 1c) search the storage unit and transmit the results to the management system (2). This system (2) acquires the route of the traced packet from the results of the search and the construction information on the network.

[続葉有]

WO 02/089426 A1

(81) 指定国 (国内): JP, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

(57) 要約:

本発明の目的は、既存のネットワーク機器を利用したままでもパケットを追跡することのできるパケット追跡システムを提供することにある。パケットプリンティング装置１ａ、１ｂ、１ｃは監視対象ネットワークに流れるすべてのパケットからハッシュ値を生成し、生成したハッシュ値を記憶部に記憶している。ＩＤＳ３は、監視対象のネットワークの不審なパケットを検知する。管理システム２は、ＩＤＳ３からの警報と追跡対象のパケットを受信すると、そのパケットのハッシュ値を生成し、パケットプリンティング装置１ａ、１ｂ、１ｃに生成したハッシュ値を含む検索要求を送信する。パケットプリンティング装置１ａ、１ｂ、１ｃは、記憶部内を検索し、結果を管理システム２に送信する。管理システム２は、検索結果と、ネットワークの構成情報から、追跡対象のパケットの経路を得る。

明 細 書

パケット追跡システム

技術分野

本発明は、既存のネットワーク機器を利用したままでもパケットの経路を追跡することのできるパケット追跡システムに関するものである。

本出願は日本国への特許出願（特願２００１－１３３２９０）に基づくものであり、当該日本出願の記載内容は本明細書の一部として取り込まれるものとする。

背景技術

従来から通信ネットワーク内の不審なパケットを検出するために、ＩＤＳ（Intrusion Detection System／侵入検知装置）が使用されている。ＩＤＳにより不審なパケットを検知し、そのパケットの追跡を行なう場合、発信元アドレスをキーとしてパケットの追跡を行なう。そのため、発信元アドレスが詐称されていると、正確なパケットの追跡ができない。このような発信元の詐称されたパケットを特定し、追跡するために、パケット内に目印となる情報を付与する等、パケットに手を加える方法や、パケットの中身を精査する方法が考えられている。

しかし、上述したパケット内に目印となる情報を付与する従来の方法は、その中身を調べるため、プライバシを侵害するという問題がある。また、第三者によってパケット内に追跡するためとして付与された情報が、悪意ある第三者によって付与された、若しくは変更された欺瞞情報である場合、そのパケットを正確に追跡することができない。

また、ルータ等、既存のネットワーク機器において追跡する方法も考えられる。しかし、この方法を実現するには、対象となるネットワーク装置内部の仕組みや、ネットワークの構成を一部変更しなければならない。そのため、機器の追加、設置場所変更等の構成変更を柔軟に行なうことができなくなる。

発明の開示

本発明の目的は、既存のネットワーク機器を利用したままでもパケットの経路を追跡することのできるパケット追跡システムを提供することにある。

本発明の要旨は、監視対象の通信ネットワークを構成する通信回線の要所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線とは物理的に異なる通信回線を介して接続された管理システムとからなり、前記パケットプリンティング装置は、監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、前記管理システムは、追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得る。

また、本発明の要旨は、監視対象の通信ネットワークを構成する通信回線の要所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線と物理的及び論理的に同一の通信回線を介して接続された管理システムとからなり、前記パケットプリンティング装置は、監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、前記管理システムは、追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得る。

また、本発明の要旨は、監視対象の通信ネットワークを構成する通信回線の要

所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線と物理的に同一で論理的に異なる通信回線を介して接続された管理システムとからなり、前記パケットプリンティング装置は、監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、前記管理システムは、追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、前記パケット特定情報を含む検索要求を、前記パケットプリンティング装置に送信し、各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得る。

この構成によれば、既存のネットワーク機器を利用したまま、パケットの通過経路を追跡することができる。

また、本発明の要旨は、前記管理システムは、前記検索要求を全ての前記パケットプリンティング装置に対して送信し、検索結果を全てのパケットプリンティング装置から受信する。

この構成によれば、検索要求処理を簡単にすることができる。

また、本発明の要旨は、前記管理システムは、前記侵入検知装置の直近に接続されるパケットプリンティング装置にのみ検索要求を行い、前記パケットプリンティング装置は、検索要求を受信した時点で検索動作を行うとともに、自己の直近に接続される他のパケットプリンティング装置に対して検索要求を行う。

この構成によれば、検索処理の効率を向上させることができる。

また、本発明の要旨は、前記管理システムは、前記侵入検知装置の直近に接続されるパケットプリンティング装置から順次検索要求を送信し、この検索要求に対する検索結果が追跡対象パケット通過したことを示すものである場合に、さらに追跡対象パケットが通過したパケットプリンティング装置の直近に接続されるパケットプリンティング装置に対して検索要求を送信する。

この構成によれば、検索処理の効率を向上させることができる。

また、本発明の要旨は、前記パケットプリンティング装置は、検索要求を受信した場合に、前記記憶部に記憶されている全てのパケット特定情報を読み出して検索を行う。

この構成によれば、検索処理を簡単にすることができる。

また、本発明の要旨は、前記管理システムは、パケット通過時刻の範囲を含む検索要求を送信し、前記パケットプリンティング装置は、受信した検索要求に含まれるパケット通過時刻の範囲内のパケット特定情報のみを前記記憶部より読み出して検索を行う。

この構成によれば、検索効率を向上させることができる。

また、本発明の要旨は、前記記憶部は、記憶しているパケット特定情報が予め決められた記憶容量を超えた場合に、最も古いパケット特定情報を破棄して、新たなパケット特定情報を記憶する。

この構成によれば、記憶部が所定の記憶容量であってもオーバーフローの発生を防止することができる。

また、本発明の要旨は、前記パケットプリンティング装置は、外部記憶装置をさらに備え、前記管理システムからの指示を受けて、前記記憶部に記憶されているパケット特定情報を前記外部記憶装置へコピーする。

この構成によれば、必要に応じてパケット特定情報を取得することができる。

また、本発明の要旨は、前記パケット特定情報は、メッセージダイジェストである。

この構成によれば、パケット特定情報を記憶する記憶部の容量を小さくすることができる。さらに、記憶部の容量が小さくなることにより、ソートや検索の効率を大幅に向上させることができる。

また、本発明の要旨は、前記メッセージダイジェストは、パケットのあらかじめ定められた部分のデータに対して生成される。

この構成によれば、パケットプリンティング装置を通過した時のパケットが、ネットワークを経由して行き、侵入検知装置がこのパケットを発見した時には、同じ内容をもつパケットにも関わらずヘッダと呼ばれる制御情報の一部がわずかに異なることがあるが、その場合でもより精度の高いパケット特定情報を生成す

ることができる。また、同じ内容のパケットが複数送信された場合、それらを同一とみなすことにより、パケット特定情報を記憶する記憶部の容量を有効に使用することができる。さらに、記憶部の容量が小さくなることにより、ソートや検索の効率を大幅に向上させることができる。

また、本発明の要旨は、前記メッセージダイジェストは、複数に分割されたパケットを結合し、この結合されたパケットから生成される。

この構成によれば、パケット特定情報を記憶する記憶部の容量を、さらに有効に使用することができる。さらに、記憶部の容量が小さくなることにより、ソートや検索の効率を大幅に向上させることができる。

また、本発明の要旨は、前記パケット特定情報は、前記通信回線を通過したパケットに対して加工を全く加えない状態のパケットである。

この構成によれば、パケット特定情報生成処理を簡単にすることができる。

また、本発明の要旨は、監視対象の通信ネットワークを構成する通信回線の要所に設置されるパケットプリンティング装置であって、前記パケットプリンティング装置は、監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、外部からの検索要求に含まれるパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を出力する。

また、本発明の要旨は、監視対象の通信ネットワークを構成する通信回線の要所に設置されるパケットプリンティング装置から出力される追跡対象パケット検索結果に基づきパケット通過経路を得る管理システムであって、前記管理システムは、追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得る。

図面の簡単な説明

図１は、本実施形態のパケット追跡システムの概要を説明するブロック図であ

る。

図２は、本実施形態のパケットプリンティング装置の構成を示すブロック図である。

図３は、本実施形態のパケットプリンティング装置の動作を説明するフローチャートである。

図４は、本実施形態の管理システムの構成を示すブロック図である。

図５は、本実施形態のパケット追跡システム構成を説明するブロック図である。

図６は、本実施形態の管理システム及びパケット追跡システムの動作を説明する図である。

図７は、本実施形態の直近のパケットプリンティング装置を説明する図である。

発明を実施するための最良の形態

まず、図１を参照して、本実施形態の概要について説明する。ネットワークＡ、Ｂ、Ｃは、イントラネット内のネットワークである。ネットワークＢ、及びＣは、ネットワークＡを介して互いに接続されている。また、ネットワークＡは、プロバイダサーバ（図示略）を介してインターネットに接続されている。

各々のネットワーク間の接続リンクには、パケットプリンティング装置１が接続されている。ここでは、各々のパケットプリンティング装置１を区別するために、パケットプリンティング装置１ａ、１ｂ、１ｃという。パケットプリンティング装置１ａ、１ｂ、１ｃは管理用ネットワークにも接続されている。パケットプリンティング装置１ａ、１ｂ、１ｃは、各々が接続されているネットワーク間の接続リンクを監視の対象とし、その監視対象ネットワークを通過するパケットのコピーを取り、コピーしたパケットを一意に特定する情報としてメッセージダイジェストを生成し、記憶している。本実施形態では、メッセージダイジェストをハッシュ値として説明する。

ＩＤＳ３はネットワークＣに接続され、ネットワークＣ内に侵入した不審なパケットの検知を行う。

管理システム２は、ネットワークの構成情報を記憶しており、ＩＤＳ３と近接し、接続されている。また、管理システム２は、パケットプリンティング装置１

ａ、１ｂ、１ｃと管理用ネットワークを介して通信することができる。

ＩＤＳ３が、ネットワークＣ内で不審なパケットを検知したものとする。ＩＤＳ３は、警報と、追跡対象の不審なパケットを管理システム２に送信する。

管理システム２は、ＩＤＳ３からの警報と、追跡対象のパケットを受信すると、受信したパケットからハッシュ値を生成する。なお、ハッシュ値の代わりにパケットそのもののコピーあるいはパケットを一意に特定することが可能なデータを含むパケットデータの一部でもよい。すなわち、受信したパケットを特定することができるデータであれば何でもよい。

次に、管理システム２は、パケットプリンティング装置１の位置を確認し、ネットワークに余計な負荷がかからないように生成したハッシュ値を含む検索要求を送信する。ここでは、パケットプリンティング装置１ａ、１ｂ、１ｃすべてに生成したハッシュ値を含む検索要求を送信するものとする。

パケットプリンティング装置１ａ、１ｂ、１ｃは、受信したハッシュ値と一致するハッシュ値を記憶しているかどうか検索する。検索が終わると、結果を管理システム２に送信する。

管理システム２は、パケットプリンティング装置１ａ、１ｂ、１ｃから送信された結果と、ネットワークの構成情報とから、パケットの経路を得る。例えば、パケットプリンティング装置１ｂ、１ｃから、一致するハッシュ値を記憶しているという結果を受信した場合、不審なパケットは、ネットワークＡを介してインターネットからきたものとなる。管理システム２は、このような結果をネットワーク管理者等に通知する。ネットワーク管理者等は、結果から、不審なパケットが通過したプロバイダサーバの管理者等に報告等する。これにより、セキュリティの防御が図られる。

なお、各ネットワークを構成する通信回線は、有線または無線で構成される。

以下、図面を参照し、本実施形態について詳細に説明する。図２は、パケットプリンティング装置１（１ａ、１ｂ、１ｃ）の内部構成を機能展開して示したブロック図である。図３は、パケットプリンティング装置１の動作を説明するものである。以下、パケットプリンティング装置１の構成、及び動作を、図２、図３を参照して説明する。

１１はタッピング装置である。タッピング装置１１は、接続する監視対象ネットワークを通過するパケットのコピーを作成する（図３におけるＳ６１）。本実施形態では、監視対象ネットワークとの接続は、ＩＰアドレス等の論理接続を持たないステルス接続であるものとする。

１２はプリンティング制御部である。プリンティング制御部１２は、あらかじめ、ハッシュ値を生成する方式（ハッシュ関数）を、パケットプリンティング部１３に指示しておく。

１３は、パケットプリンティング部である。パケットプリンティング部１３は、プリンティング制御部１２に指示された方式（ハッシュ関数）で、タッピング装置１１がコピーしたパケットのハッシュ値を生成する（図３におけるＳ６２）。

１４はキャッシュ制御部である。キャッシュ制御部１４は、キャッシュ部１５に記憶されているハッシュ値の量（個数）を認識する（図３におけるＳ６３）。キャッシュ部１５に記録されているハッシュ値が一定量以上であった場合、キャッシュ制御部１４は、キャッシュ部１５に記憶されている最も古いハッシュ値を破棄する（図３におけるＳ６４）。キャッシュ部１５に記録されているハッシュ値が一定量以下であった場合、キャッシュ制御部１４は、キャッシュ部１５に記憶されている情報の最後尾に新しいハッシュ値を追加して記憶する。

このように、キャッシュ制御部１４は、キャッシュ部１５に記憶されているハッシュ値が常に一定量以下になるよう制御する。また、すべてのパケットのヘッダ部分には、当該パケットの寿命を示すＴＴＬ（Time To Live）が付随している。キャッシュ制御部１４は、ハッシュ値を、当該パケットが通過した時間を示すタイムスタンプと、ＴＴＬとを関連付けてキャッシュ部１５の空いているフィールド等に記憶させる（図３におけるＳ６５）。

パケットプリンティング装置１は、監視対象ネットワークを通過するすべてのパケットに対し、上述の動作を行っている。１６は追跡エージェント部であり、管理ネットワークとＩＰ接続され、管理システム２と通信する。追跡エージェント部１６の動作については、後述する管理システム２の動作のところで説明する。

なお、本実施形態では、監視対象ネットワークと管理用ネットワークは、互いに独立して存在するものとする。これにより、監視対象ネットワークからの侵入

者に、パケットプリンティング装置１の存在を気づかれない。

次に、管理システム２について、図面を参照して説明する。図４は、管理システム２の構成を示すブロック図である。この図において、２１は警報受信部であり、接続されているＩＤＳ３から不審なパケットに対する警報を受信する。２２はパケット受信部であり、接続されているＩＤＳ３から不審なパケットを受信する。

２３はプリンティング制御部であり、あらかじめ、ハッシュ値を生成する方式（ハッシュ関数）を、パケットプリンティング部２４に指示しておく。

パケットプリンティング装置１のプリンティング制御部１２で指定される方式と、管理システム２のプリンティング制御部２３で指定される方式は常に同じである。

２４はパケットプリンティング部であり、プリンティング制御部２３に指示された方式（ハッシュ関数）で、パケット受信部２２が受信したパケットのハッシュ値を生成する。２５は追跡要求部であり、パケットプリンティング部２４で生成されたハッシュ値を含む検索要求を各パケットプリンティング装置１ａ、１ｂ、１ｃに送信し、さらに、検索結果を受信する。

２６は構成情報であり、監視対象ネットワーク及び管理用ネットワークの構成を記憶するＤＢ（データベース）である。２７は追跡経路作成部であり、パケットプリンティング装置１ａ、１ｂ、１ｃから送信された検索結果と、構成情報２６の情報とから、パケットの通過経路を作成する。

ここで、図５に示すシステム構成において、管理システム２のパケット追跡の動作を、図６を参照して説明する。

図５において、５１、５２はＩＳＰ（Internet Service Provider）である。３５は、ウェブページなどのサービスを提供するサーバである。

ＩＳＰ５１、５２、サーバ３５は、各々ルータ３１、３２、３３を介して中継されている。

ルータ３１、３２、３３が接続されているネットワークに、パケットプリンティング装置１ａ、１ｂ、１ｃが接続されている。パケットプリンティング装置１ａ、１ｂ、１ｃは、ルータ３１、３２、３３と接続されているネットワークを監

視対象ネットワークとし、各ルータを通過するすべてのパケットのハッシュ値を生成し、記憶している。なお、本実施形態では、パケットプリンティング装置１ａ、１ｂ、１ｃは、ＮＴＰ同期（Network Time Protocol）により、内部時計の時刻を同期させているものとする。

ＩＤＳ３はサーバ３５と接続されているものとする。ＩＤＳ３はサーバ３５の不審なパケットを監視している。管理システム２は、ＩＤＳ３と近接し、接続されている。

パケットプリンティング装置１ａ、１ｂ、１ｃ、管理システム２、ＩＤＳ３は、管理用ネットワーク（図示略）にＩＰ接続されているものとする。

いま、ＩＤＳ３が、不審なパケットをサーバ３５内から検出したとする。ＩＤＳ３は、不審なパケットに対する警報を管理システム２に送信する。管理システム２は、警報受信部２１で警報を受信する。警報を受信すると、管理システム２は、警報の対象となったパケットの送信をＩＤＳ３に要求する。要求を受けたＩＤＳ３は、追跡対象となる不審なパケットそのものを管理システム２に送信する。管理システム２のパケット受信部２２は追跡対象のパケットを受信する（図６におけるＳ７１）。

プリンティング制御部２３は、あらかじめ、ハッシュ値を生成する方式（ハッシュ関数）を、パケットプリンティング部２４に指示しておく。パケットプリンティング部２４は、パケット受信部２２で受信したパケットから、プリンティング制御部２３に指示されたハッシュ関数を利用してハッシュ値を生成する（図６におけるＳ７２）。

追跡要求部２５は、構成情報２６を参照し、パケットプリンティング装置１の位置と数とを確認し、検索要求を送信するパケットプリンティング装置１を決定する（図６におけるＳ７３）。近くにあるパケットプリンティング装置１の数が少ない場合、追跡要求部２５は、近くにあるすべてのパケットプリンティング装置１に、生成したハッシュ値を含む検索要求を送信する。近くにあるパケットプリンティング装置１の数が多い場合、追跡要求部２５は、最も近くにあるパケットプリンティング装置１から順に、生成したハッシュ値を含む検索要求を送信する。本実施形態では、パケットプリンティング装置１ｃに検索要求を送信したも

のとする。

パケットプリンティング装置１ｃの追跡エージェント部１６は、検索要求を受信する（図６におけるＳ７４）。次に、追跡エージェント部１６は、キャッシュ部１５を参照し、受信したハッシュ値と同じハッシュ値を記憶しているか検索する（図６におけるＳ７５）。そして、受信したハッシュ値と同じハッシュ値を記憶していれば「真」、記憶していなければ「偽」を、管理システム２の追跡要求部２５に送信する（図６におけるＳ７６）。

また、キャッシュ部に該当するハッシュ値を記憶していれば、パケットプリンティング装置１ｃの追跡エージェント部１６は、ハッシュ値と関連付けられて記憶されているタイムスタンプとＴＴＬを含む検索結果を管理システム２に送信する。

本実施形態では、パケットプリンティング装置１ｃは「真」という結果を管理システム２に送信したものとする。

管理システム２の追跡要求部２５は検索結果を受信する。追跡経路作成部２７は、検索結果と、構成情報２６に記憶されているネットワーク構成の情報とを比較することにより、追跡対象のパケットの通過経路情報を作成する。

本実施形態では、パケットプリンティング装置１ｃから、「真」という検索結果を受信したので、ＩＤＳ３からパケットプリンティング装置１ｃの間を通過経路とする（図６におけるＳ７７）。

なお、パケットプリンティング装置１ｃから、「偽」という検索結果を受信した場合、不審なパケットはサーバ３５本体、あるいは、サーバ３５と接続された端末等（図示略）からのパケットなので、本システムによるパケットの通過経路追跡は終了する。

次に、管理システム２の追跡要求部２５は、構成情報２６を参照し、パケットプリンティング装置１ｃの近くに設置されており、かつ、まだ検索要求を送信していないパケットプリンティング装置１があるか検索する（図６におけるＳ７８）。その検索の結果、まだ検索要求を送信していないパケットプリンティング装置１ａ、１ｂが検索される。そこで、追跡要求部２５は、パケットプリンティング装置１ｃの近くに設置されているパケットプリンティング装置１ｂに検索要

求を送信する。

パケットプリンティング装置１ｂは、キャッシュ部１５を検索し、結果を送信する。本実施形態では、「偽」という結果が送信されたものとする。

パケットプリンティング装置１ｂから「偽」という検索結果を受信した管理システム２の追跡要求部２５は、上述したパケットプリンティング装置１の検索を行い、パケットプリンティング装置１ａに対し検索要求を送信する。

パケットプリンティング装置１ａは、キャッシュ部１５を検索し、結果を送信する。本実施形態では、「真」という結果が送信されたものとする。

パケットプリンティング装置１ａから、「真」という検索結果を受信した管理システム２の追跡経路作成部２７は、パケットプリンティング装置１ｃからパケットプリンティング装置１ａの間を、不審なパケットの通過経路とする。

次に、追跡要求部２５は、上述したパケットプリンティング装置１の検索を行う。検索要求を送信していないパケットプリンティング装置１が検出されないので、経路の追跡を終了する。

上述の動作により得られたパケットの通過経路情報を、追跡経路作成部２７は、ネットワーク管理者等へのレポートにして通知する。不審なパケットの通過経路がパケットプリンティング装置１ｃからパケットプリンティング装置１ａの間であることから、不審なパケットはＩＳＰ５１から来たものと判断できる。ネットワーク管理者は、ＩＳＰ５１の管理者に報告するなどして、不審なパケットに対する対策を打つことができる。

なお、構成情報２６の情報、あるいはパケットプリンティング装置１の設置が十分でないときも、ハッシュ値と関連付けられているタイムスタンプ、及びＴＴＬとから、大体の経路を割り出すことができる。

本実施形態において、パケットプリンティング装置１、及び、管理システム２がハッシュ値を生成するのに使用する方式（ハッシュ関数）はＭＤ５等でもよく、他の方式でもよい。ここで、本実施形態で使用可能な、ハッシュ値を生成する方式のバリエーションについて説明する。

１．同一のパケットの場合

ＤｏＳ攻撃（Denial of Service）等の、同一のパケットを大量に送信する攻撃

を受けた場合に有効な方式について説明する。

パケットは、簡単にあらわすと、ヘッダ部分と本体部分から成る。同じ内容のパケットでも、ヘッダ部分はパケットの通過経路等により、パケット毎に異なる。従って、パケット全体からハッシュ値を生成した場合、同じ本体部分を持つパケットでも、異なるハッシュ値が得られる場合がある。そこで、ヘッダ構成要素のうち、例えば、「識別番号」、「ＴＴＬ」、「ヘッダチェックサム」のような、パケット毎に異なる部分を除いた部分からハッシュ値を生成すると、同一の本体部分を持つパケットのハッシュ値は同一となる。

パケットプリンティング装置１は前述の方式でハッシュ値を生成している。同一のハッシュ値を連続して生成していると判断した場合、以降生成した同一のハッシュ値を、記憶せずに破棄するようにする。

２．パケットの結合

通常、一つのオペレーションに関するデータは、複数のパケットに分割され、伝送される。このように、複数に分割されたパケットを結合し、結合されたパケットからハッシュ値を生成する方法も考えられる。この結合の方法としては以下のようなことが考えられる。

①複数のパケットを、セッション単位（オペレーション単位）で単純に結合する。

②「識別番号」、「ＴＴＬ」、「ヘッダチェックサム」等の、パケット毎に異なる部分を除いたヘッダ部分と内容を結合する。

③先頭パケットのヘッダ部分と、すべてのパケットの内容部分を結合する。

上記のような方法で結合したパケットからハッシュ値を生成することで、パケットをセッション単位で記録することができる。

上述１、２に例を示すハッシュ関数のバリエーションを利用することにより、パケットプリンティング装置１のキャッシュ部１５の容量を小さくすることが可能となる。さらに、キャッシュ部１５の容量が小さくなることにより、ソートや検索の効率を大幅に向上させることができる。また、上述１に例を示すハッシュ関数のバリエーションは、より精度の高いパケット特定情報を生成するという利点もある。

次に、図７を参照して、管理システム２が検索要求を送信して、この検索要求に対してパケットプリンティング装置１が検索結果を返す場合の送信先を決定する動作を説明する。この図において、符号Ｎは、監視用ネットワークであり、各ルータ３４、３５に接続される。符号１－１～７は、監視用ネットワークＮにそれぞれ接続されたパケットプリンティング装置である。各パケットプリンティング装置１－１～７は、管理ネットワークを介して管理システム２へ接続される。

（ａ）全てのパケットプリンティング装置に対して検索要求を送信する場合

管理システム２は、ＩＤＳ３から通知されたパケット特定情報を含む検索要求を管理ネットワークを介して、全てのパケットプリンティング装置１－１～７へ送信し、この検索要求を受信したパケットプリンティング装置１－１～７は、内部を検索して、その結果を管理システム２へ送信する。

（ｂ）ＩＤＳの直近のパケットプリンティング装置のみに対して検索要求を送信する場合

管理システム２は、ＩＤＳ３から通知されたパケット特定情報を含む検索要求を管理ネットワークを介して、ＩＤＳ３の直近のパケットプリンティング装置１－５のみに送信する。これを受けたパケットプリンティング装置１－５は、自己の直近に位置するパケットプリンティング装置１－１，１－２，１－４に対して、検索要求を送信する。自己の直近の装置は予め各パケットプリンティング装置１－１～７内に記憶されている。これを受けたパケットプリンティング装置１－１，１－２，１－４は、検索対象のパケット特定情報の検索結果を、この検索要求を送信したパケットプリンティング装置１－５に対して通知する。そして、パケットプリンティング装置１－１，１－２，１－４のそれぞれは、自己内に検索対象のパケット特定情報が記憶されていた場合のみ、さらに自己の直近に位置するパケットプリンティング装置１－３、１－６、１－７へ検索要求を送信する。この動作を繰り返し行うことにより、検索対象のパケットの通過経路を追跡し、パケットプリンティング装置１－５が検索結果をとりまとめて管理システム２へ送信する。このようにすることにより、管理システム２は、１つのパケットプリンティング装置１－５のみに検索要求を行うだけでパケットの追跡を行うことが可能となる。また、検索対象のパケット特定情報が記憶されていた場合にのみさらに

直近のパケットプリンティング装置１に対して検索要求を行うようにしたため、検索効率を向上させることが可能となる。

（ｃ）パケットの通過が確認されたときのみさらに検索要求を送信する場合

管理システム２は、ＩＤＳ３から通知されたパケット特定情報を含む検索要求を管理ネットワークを介して、ＩＤＳ３の直近のパケットプリンティング装置１－５のみに送信する。そして、この検索要求を送信したパケットプリンティング装置１－５内に検索対象のパケット特定情報が記憶されていた場合のみ、さらに、管理システム２は、パケット特定情報が記憶されていたパケットプリンティング装置１－５の直近する装置に対して検索要求を行い、検索結果を受信する。管理システム２内には、各パケットプリンティング装置１の直近の装置が予め定義されている。この動作を繰り返し行うことによって検索対象のパケットの通過経路を追跡する。このように、検索対象のパケット特定情報が記憶されていた場合にのみさらに直近のパケットプリンティング装置１に対して検索要求を行うようにしたため、検索効率を向上させることが可能となる。

なお、上述の方式によりパケットを特定する情報を得ても、あるいは他の方法でパケットを特定する情報を得てもよい。要は、パケットそのものを加工したり、内容を精査する事なく一意に特定できる情報を得ることができればよい。

また、上述の実施形態では、監視対象ネットワークと管理用ネットワークは、互いに独立して存在するものとした。しかし、これに限られるわけでなく、パケットプリンティング装置１の追跡エージェント部１６は、監視対象ネットワークに接続されており、管理システム２からのパケット検索要求を、監視対象ネットワーク経由で送信してもよい。要は、パケットプリンティング装置１と管理システム２とが、通信ネットワークにより接続されていればよく、物理的に同一な通信回線で、論理的に異なる通信回線であってもよい。さらに、管理ネットワークと監視ネットワークは、物理的に同一でかつ論理的にも同一の通信回線であってもよい。

また、上述の実施形態では、管理システム２は、ＩＤＳから不審なパケットに対する警報を受信し、次に、追跡対象となる不審なパケットそのものを受信するとした。しかし、不審なパケットに対する警報と、不審なパケットそのものを同

時に受信してもよい。

また、上述の本実施形態では、パケットプリンティング装置１ａ、１ｂ、１ｃは、ＮＴＰ同期（Network Time Protocol）により、内部時計の時刻を同期させているものとしたが、これに限られるわけではない。同期をとる方法として、ＧＰＳクロック等を用いてもよい。

また、パケット特定情報を各パケットプリンティング装置１ａ、１ｂ、１ｃ内に全て記憶しておき、一定期間毎に各パケットプリンティング装置１ａ、１ｂ、１ｃ内に記憶しておいたパケット特定情報を管理システム２へ送信するようにしてもよい。このとき、一定期間に監視対象ネットワークを通過するパケット量を見積っておき、各パケットプリンティング装置１ａ、１ｂ、１ｃには、見積もったパケット量を全て記憶しておける外部記憶装置を備えるようにしておく。

また、各パケットプリンティング装置１ａ、１ｂ、１ｃは、パケット特定情報を記憶する場合に、パケット通過時刻を合わせて記憶するようにして、管理システム２から通過時刻の範囲を限定して検索要求された場合に、この検索時間範囲内で検索するようにしてもよい。このようにすることによって、不審なパケットの通過時刻に基づく検索が可能となるために、検索に必要な時間を削減することが可能となり、パケット追跡を素早く行うことが可能となる。

さらに、パケット追跡の必要が生じた時に外部からのトリガに基づいて、各パケットプリンティング装置１ａ、１ｂ、１ｃ内に記憶しておいたパケット特定情報を記憶容量の大きい記録媒体に記録するようにしてもよい。さらに、管理用ネットワークを設けずに、記憶容量の大きい記録媒体から可搬な記録媒体に記録して、この記録媒体を管理システム２に対して手渡すようにしてもよい。

また、各パケットプリンティング装置１ａ、１ｂ、１ｃは、ＩＤＳ３の機能を有していてもよい。これにより、管理システム２からの要求に基づくのではなく、自ら不審なパケットを検出し、不審なパケットが検出された時点で管理システムへ通知することが可能となる。

また、図２、及び図４における各部の機能の一部またはすべてを実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行させること

により実現させてもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計変更等も含まれる

請 求 の 範 囲

1. 監視対象の通信ネットワークを構成する通信回線の要所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線とは物理的に異なる通信回線を介して接続された管理システムとからなり、

前記パケットプリンティング装置は、

監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、

前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、

前記管理システムは、

追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、

前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、

各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得ることを特徴とするパケット追跡システム。

2. 監視対象の通信ネットワークを構成する通信回線の要所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線と物理的及び論理的に同一の通信回線を介して接続された管理システムとからなり、

前記パケットプリンティング装置は、

監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、

前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、

前記管理システムは、

追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、

前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、

各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得ることを特徴とするパケット追跡システム。

3. 監視対象の通信ネットワークを構成する通信回線の要所に各々複数設置されたパケットプリンティング装置と、前記各パケットプリンティング装置に対して前記通信回線と物理的に同一で論理的に異なる通信回線を介して接続された管理システムとからなり、

前記パケットプリンティング装置は、

監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、

前記管理システムからの要求を受けて該管理システムから送信されたパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を前記管理システムへ送信し、

前記管理システムは、

追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、

前記パケット特定情報を含む検索要求を、前記パケットプリンティング装置に送信し、

各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得ることを特徴とするパケット追跡システム。

4. 前記管理システムは、前記検索要求を全ての前記パケットプリンティング装置に対して送信し、検索結果を全てのパケットプリンティング装置から受信する請求の範囲第1項～第3項のいずれかに記載のパケット追跡システム。

5． 前記管理システムは、前記侵入検知装置の直近に接続されるパケットプリンティング装置にのみ検索要求を行い、前記パケットプリンティング装置は、検索要求を受信した時点で検索動作を行うとともに、自己の直近に接続される他のパケットプリンティング装置に対して検索要求を行う請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

6． 前記管理システムは、前記侵入検知装置の直近に接続されるパケットプリンティング装置から順次検索要求を送信し、この検索要求に対する検索結果が追跡対象パケット通過したことを示すものである場合に、さらに追跡対象パケットが通過したパケットプリンティング装置の直近に接続されるパケットプリンティング装置に対して検索要求を送信する請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

7． 前記パケットプリンティング装置は、検索要求を受信した場合に、前記記憶部に記憶されている全てのパケット特定情報を読み出して検索を行う請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

8． 前記管理システムは、パケット通過時刻の範囲を含む検索要求を送信し、前記パケットプリンティング装置は、受信した検索要求に含まれるパケット通過時刻の範囲内のパケット特定情報のみを前記記憶部より読み出して検索を行う請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

9． 前記記憶部は、記憶しているパケット特定情報が予め決められた記憶容量を超えた場合に、最も古いパケット特定情報を破棄して、新たなパケット特定情報を記憶する請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１０． 前記パケットプリンティング装置は、外部記憶装置をさらに備え、前記

管理システムからの指示を受けて、前記記憶部に記憶されているパケット特定情報を前記外部記憶装置へコピーする請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１１．　前記パケット特定情報は、メッセージダイジェストである請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１２．　前記メッセージダイジェストは、パケットのあらかじめ定められた部分のデータに対して生成される請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１３．　前記メッセージダイジェストは、複数に分割されたパケットを結合し、この結合されたパケットから生成される請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１４．　前記パケット特定情報は、前記通信回線を通過したパケットに対して加工を全く加えない状態のパケットである請求の範囲第１項～第３項のいずれかに記載のパケット追跡システム。

１５．　監視対象の通信ネットワークを構成する通信回線の要所に設置されるパケットプリンティング装置であって、

前記パケットプリンティング装置は、

監視対象の通信回線を通過するパケットのそれぞれについて、該パケットを特定するパケット特定情報を生成して記憶部に記憶させ、

外部からの検索要求に含まれるパケット特定情報と同一の情報が前記記憶部にあるか否かを検索し、その結果を出力するパケットプリンティング装置。

１６．　監視対象の通信ネットワークを構成する通信回線の要所に設置されるパケットプリンティング装置から出力される追跡対象パケット検索結果に基づきパ

ケット通過経路を得る管理システムであって、

前記管理システムは、

追跡対象のパケットから、該パケットを特定するパケット特定情報を生成し、

前記パケット特定情報を含む検索要求を、複数の前記パケットプリンティング装置に送信し、

各パケットプリンティング装置から受信された検索結果と、予め内部の記憶部に記憶している通信ネットワークの構成に関する情報とから、追跡対象パケットの通過経路に関する情報を得る管理システム。

図 1

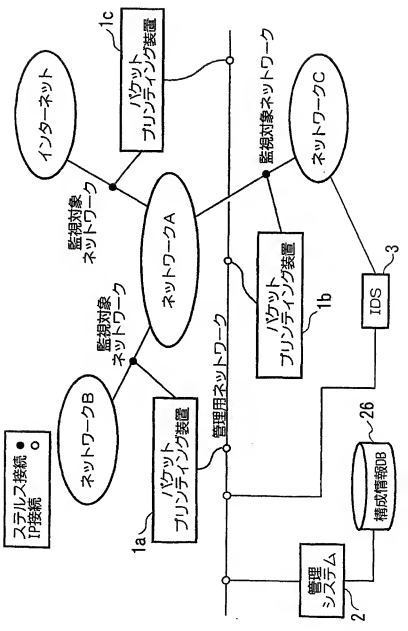

ステルス接続 ●
IP接続 ○
ネットワークB
監視対象ネットワーク
パケットブリッティング装置
1a
管理用ネットワーク
ネットワークA
監視対象ネットワーク
インターネット
パケットブリッティング装置
1c
パケットブリッティング装置
1b
監視対象ネットワーク
ネットワークC
IDS
3
構成情報DB
26
管理システム
2

図２

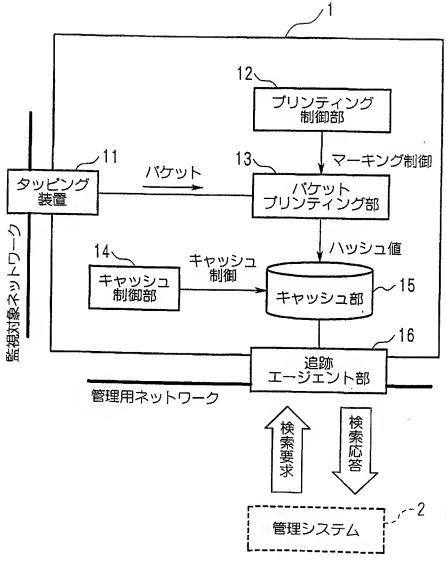

1
12
プリンティング制御部
11
タッピング装置
バケット
13
マーキング制御
バケットプリンティング部
ハッシュ値
14
キャッシュ制御部
キャッシュ制御
キャッシュ部
15
16
追跡エージェント部
監視対象ネットワーク
管理用ネットワーク
検索要求
検索応答
管理システム
2

図３

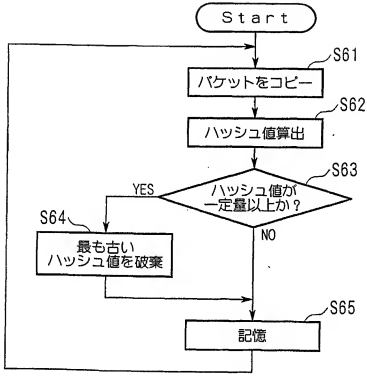

Start
S61
パケットをコピー
S62
ハッシュ値算出
S63
ハッシュ値が
一定量以上か？
YES
NO
S64
最も古い
ハッシュ値を破棄
S65
記憶

図4

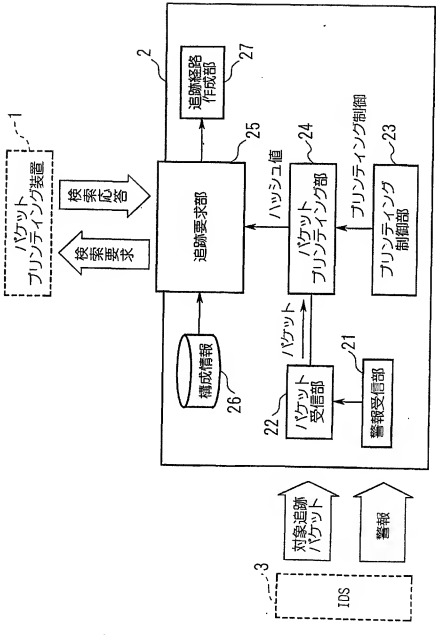

パケット
プリンティング装置
1
検索応答
検索要求
追跡要求部
25
2
追跡経路
作成部
27
ハッシュ値
パケット
プリンティング部
24
プリンティング制御
プリンティング
制御部
23
構成情報
26
パケット
22
パケット
受信部
21
警報受信部
対象追跡
パケット
警報
IDS
3

図5

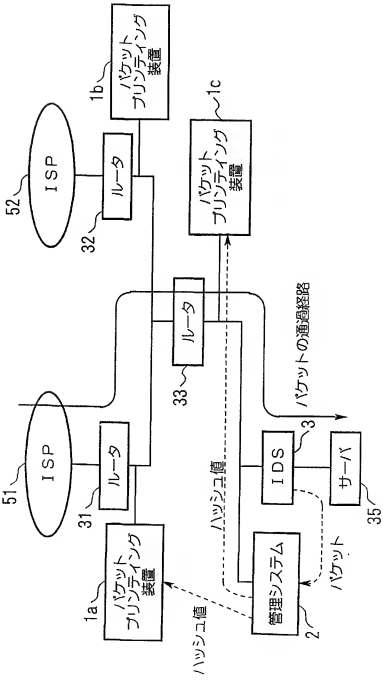

ISP
51
ルータ
31
パケット
プリンティング
装置
1a
ISP
52
ルータ
32
パケット
プリンティング
装置
1b
ルータ
33
パケット
プリンティング
装置
1c
IDS
3
サーバ
35
管理システム
2
ハッシュ値
ハッシュ値
パケット
パケットの通過経路

図６

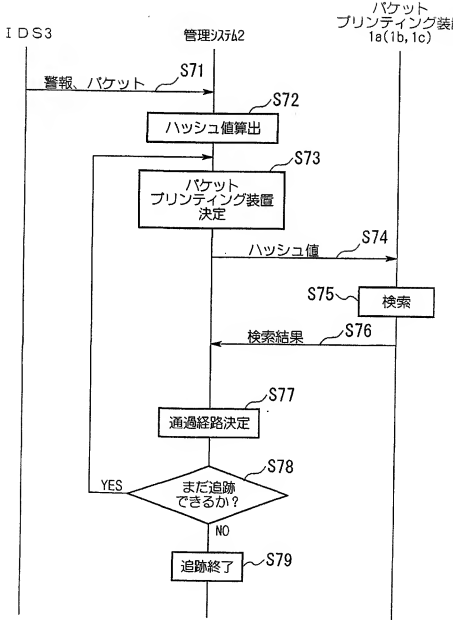
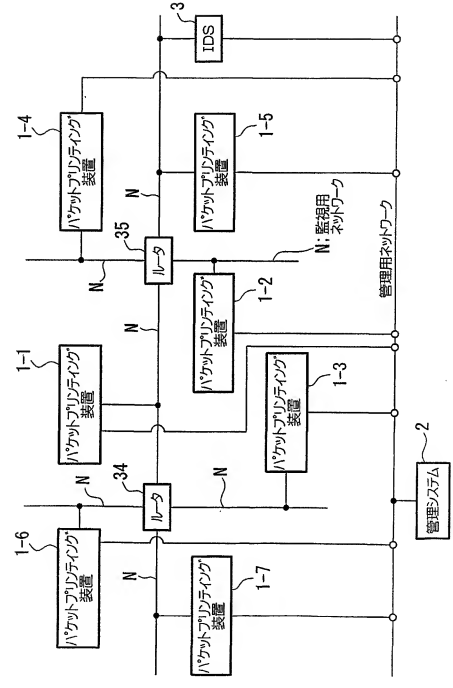

ＩＤＳ3
管理ｼｽﾃﾑ2
パケット
プリンティング装置
1a(1b,1c)
S71
警報、パケット
S72
ハッシュ値算出
S73
パケット
プリンティング装置
決定
S74
ハッシュ値
S75
検索
検索結果
S76
S77
通過経路決定
S78
YES
まだ追跡
できるか？
NO
追跡終了
S79

図 7


3
IDS
1-4
パケットプリンティング装置
1-5
パケットプリンティング装置
35
N
ルータ
N
N: 監視用ネットワーク
管理用ネットワーク
1-2
パケットプリンティング装置
1-1
パケットプリンティング装置
1-3
パケットプリンティング装置
34
ルータ
1-6
パケットプリンティング装置
1-7
パケットプリンティング装置
2
管理システム

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/04139

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl' H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl' H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE Xplore (packet* and rout* and trac*)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Katsutoshi KOKUBO et al., "Fusei Access Hasshingen Tsuiseki System no Model Kento", 14 March, 2000 (14.03.00), Information Processing Society of Japan Dai 60 Kai (First term of Heisei 12 Nen (2000)) Zenkoku Taikai Koen Ronbunshu (3), 6Q-4, pages 3-283 to 3-284	1-4,7,9, 14-16 5,8,10-13
X Y	Motoki IKEDA, "Fusei Access Hasshingen Tsuiseki System no Architecture no Yukosei Kensho", 13 March, 2001 (13.03.01), Information Processing Society of Japan Dai 62 Kai (First term of Heisei 13 Nen (2001)) Zenkoku Taikai Koen Ronbunshu (3), 1S-2, pages 3-285 to 3-286	1-3,6,7, 9,14-16 5,8,10-13
Y	JP 2000-124952 A (NTT Data Corp.), 28 April, 2000 (28.04.00), Par. Nos. [0027] to [0028]; Fig. 3 (Family: none)	5

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 May, 2002 (17.05.02)	04 June, 2002 (04.06.02)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/04139

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Alex C. Snoeren et al., Hash-Based IP Traceback, 07 February, 2000 (07.02.00), BBN Technical Memorandum No.1284, chapter 5.1 to 5.2	8,10
Y	Hidetoshi WATANABE et al., "Fusei Access Hasshingen Tsuiseki no tameno Packet Shikibetsu Joho no Kento", 14 March, 2000 (14.03.00), Information Processing Society of Japan Dai 60 Kai (First term of Heisei 12 Nen (2000)) Zenkoku Taikai Koen Ronbunshu (3), 6Q-7, pages 3-289 to 3-290	11-13
A	Hidetoshi WATANABE et al., "Fusei Access Hasshingen Tsuiseki ni okeru Packet Shikibetsu Joho no Yukosei Kensho", 03 October, 2000 (03.10.00), Information Processing Society of Japan Dai 61 Kai (Latter term of Heisei 12 Nen (2000)) Zenkoku Taikai Koen Ronbun shu (3), 4F-7, pages 3-259 to 3-260	1-16
A	Bellovin et al., ICMP Traceback messages, 2000.03, Internet Draft, draft-ietf-itrace-00.txt	1-16
T,A	Shigeyuki MATSUDA et al., Design and Inplementation of Unauthorized Access Tracing System, 28 January, 2002 (28.01.02), Proceedings of the 2002 Symposium on Applications and the Internet(SAINT' 02)	1-16
A	Yosuke TAKEI et al., "Traffic Pattern o Mochiita Fusei Access Kenshutsu oyobi Tsuiseki Hoshiki", 18 November, 1999 (18.11.99), The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyu Hokoku, IN99-75	1-16
A	Hal Burch et al., Tracing Anonymous Packets to Their Approximate Source, 03 December, 2000 (03.12.00), 2000 LISA XIV	1-16

国際調査報告	国際出願番号　PCT／JP02／04139

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl' H04L12／56

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl' H04L12／56

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－2002年
日本国登録実用新案公報　1994－2002年
日本国実用新案登録公報　1996－2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
IEEE Xplore (packet* and rout* and trac*)

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	小久保　勝敏他，不正アクセス発信源追跡システムのモデル検討，2000．03．14，情報処理学会第60回（平成12年前期） 全国大会講演論文集（3），6Q－4，第3-283頁から第3-284頁	1-4,7,9,14-16 5,8,10-13
X Y	池田　基他，不正アクセス発信源追跡システムのアーキテクチャの有効性検証，2001．03．13，情報処理学会第62回（平成13年前期）全国大会講演論文集（3），1S－2，第3-285頁から第3-286頁	1-3,6,7,9,14-16 5,8,10-13

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17．05．02	04.06.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	3047
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	吉田　隆之 電話番号　03－3581－1101　内線　3596		

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	ＪＰ　２０００－１２４９５２　Ａ（株式会社エヌ・ティ・ティ・データ），２０００．０４．２８， 第0027段落から第0028段落，第３図（ファミリーなし）	5
Y	Alex C. Snoeren他，Hash-Based IP Traceback， ２０００．０２．０７，BBN Technical Memorandum No. 1284. 第５．１章から第５．２章	8,10
Y	渡辺　英俊他，不正アクセス発信源追跡のためのパケット識別情報の検討，２０００．０３．１４，情報処理学会第６０回（平成１２年前期）全国大会講演論文集（３），６Ｑ－７， 第3-289頁から第3-290頁	11-13
A	渡辺　英俊他，不正アクセス発信源追跡におけるパケット識別情報の有効性検証，２０００．１０．０３，情報処理学会第６１回（平成１２年後期）全国大会講演論文集（３）， ４Ｆ－７，第3-259頁から第3-260頁	1-16
A	Bellovin他，ICMP Traceback messages，２０００．０３， Internet Draft，draft-ietf-itrace-00.txt	1-16
T，A	Shigeyuki Matsuda他，Design and Inplementation of Unauthorized Access Tracing System，２００２．０１．２８， Proceedings of the 2002 Symposium on Applications and the Internet (SAINT' 02)	1-16
A	武井　洋介他，トラヒックパターンを用いた不正アクセス検出及び追跡方式，１９９９．１１．１８， 電子情報通信学会技術研究報告，ＩＮ９９－７５	1-16
A	Hal Burch他，Tracing Anonymous Packets to Their Approximate Source，２０００．１２．０３，2000 LISA XIV	1-16